1. predavanje, 26.3.2021.

1. Moderna kriptografija (primjeri) je zasnovana na faktorizaciji i problemu diskretnog logaritma

Primjer 1 (RSA) (Rivest, Shamir, Adleman) 1977.

(1973 Cliff-ord Cocks) Britanska obavješ. agencija 1997. declassified GCHQ

- kriptografija javnog ključa
- asimetričnim kriptosustav (Cezarova šifra...)
- jedno smjerna funkcija

- Generiranj ključeva

1. odaberi proste brojeve p i q
2. $n := p\,q$
3. $\lambda(n) := NZV(p-1, q-1)$
4. $1 < e < \lambda(n)$ t.d. $(e, \lambda(n)) = 1$
5. $d \equiv e^{-1} \pmod{\lambda(n)}$

javni ključ: (e, n)

tajni ključ: d

Enkripcija: Alice ⟶ Bob, d ← tajni ključ

(e, n) ← javni ključ, $n = pq$

Teško je izračunati $\lambda(n)$ bez poznavanja faktorizacije broja n

poruka $0 \leq m < n$

- $c \equiv m^e \pmod{n}$ ⟶ Bob

Dekripcija: $c^d \equiv m^{ed} \equiv m \pmod{n}$

zašto?

Treba pokazati: $m^{ed} \equiv m \pmod{p}$ i $m^{ed} \equiv m \pmod{q}$

$NZV(p-1, q-1) \mid ed - 1 \Rightarrow ed \equiv 1 \pmod{p-1}$

a znamo da je $\#(\mathbb{Z}/p\mathbb{Z})^* = p-1$

Jedan napad: loš generator slučajnih brojeva

- (2012) ... faktorizirali su 0.7% ključeva s "Interneta"

  ideja: ako $n = pq$ i $n' = p \cdot q'$ onda se s Euklidovim algoritmom brzo može odrediti $p = GCD(n, n')$

- sličnu istraživanje: ali računanje $GCD(n,$ produkt svih ostalih ključeva) ↗ broj od 729 milijuna znamenki

  - značajno ubrzanje

(Nadia Heninger; New research: There's no need to panic over ...)

Primjer 2: Diffie-Hellman protokol za razmjenu ključeva

(1976) + Merkle

ali 1969. H. Ellis

C. Cocks i M. J. Williamson

Britanska obavještajna agencija

- kriptografija javnog ključa

Alice ⟷ Bob

Protokol:

1. Alice i Bob se javno dogovore oko prostog broja p i baze g (= primitivni korijen modulo p)
2. Alice odabere tajni broj a i Bobu pošalje $A = g^a \bmod p$
3. Bob odabere tajni broj b i Alici pošalje $B = g^b \bmod p$
4. Alice izračuna $s = B^a \bmod p$, a Bob izračuna $s' = A^b \bmod p$
5. $s = s'$ je njihova zajednička tajna

Uočimo: umjesto grupe $(\mathbb{Z}/p\mathbb{Z})^*$ mogli smo odabrati bilo koju abelovu grupu – dvije najpoznatije varijante

ali PRIMES in P!

- grupa točaka na eliptičkoj krivulji
- "grupa" putova na grafu supersingularnih izogenija modulo p ↓

nema dokaza

jer ga mitkor nije uspio pronaći

Sigurnost se bazira na pretpostavci da ne postoji polinomijalno (efikasno) rješenje problema diskretnog logaritma (DLP) za grupu $G = (\mathbb{Z}/p\mathbb{Z})^*$

Neka je g generator od $(\mathbb{Z}/p\mathbb{Z})^*$. Za $h \in G$ odredite $n \in \mathbb{N}$ t.d. $g^n = h$.

(ključevi: 2048 bitova za $(\mathbb{Z}/p\mathbb{Z})^*$, 256 za $E(\mathbb{F}_p)$)

2. Kvantno računanje

Shor (1994) "Algorithms for quantum computation: discrete logarithms and factoring"

↑ polinomijalni algoritam koji rješava oba problema

Naš cilj je razumjeti taj algoritam i "ešte" implementirati na IBM Q kvantnom računalu u oblaku (qiskit)

→ literatura: Kvantno računanje, skripta (na mojoj web stranici)

2.1. Uvod : Što je to kvantno računanje? Postoji li kvantno računalo? Što je to kvantna premoć?

Hoće li kvantna računala ikad moći faktorizirati brojeve od 200 znamenaka?

2.2. Osnovni pojmovi

- kvantni bit - qubit = element norme 1 u vektorskom (unitarnom) prostoru stanja $V = \langle |0\rangle, |1\rangle \rangle$ nad $\mathbb{C}$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$a, b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$

Na primjer, jedan vektor stanja je

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Koja je razlika između bita i qubita? Mjerenje.

Klasično nema potrebe govoriti o mjerenju bitova - osim
(smisla)

kod greške u memoriji, stanje bita odgovara onome što pročitamo u memoriji – bit je ili u stanju 0 ili u stanju 1

Za qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ kažemo da je u **superpoziciji** stanja $|0\rangle$ i $|1\rangle$. Kad mjerimo qubit $|\psi\rangle$ (u bazi $\{|0\rangle, |1\rangle\}$)

pojam iz kvantne mehanike

projektivno mjerenje

s vjerojatnošću $|a|^2$ dobit ćemo rezultat $|0\rangle$

... ... $|b|^2$ ... $|1\rangle$

$(|a|^2 + |b|^2 = 1)$

- Fizikalna realizacija qubita.

- kvantna sprezanja (quantum entanglement)

Kako opisati sustav od n qubita?

prostor stanja = $V^{\otimes n} = V \otimes V \otimes \dots \otimes V$ ← $\dim = 2^n$

← unitarni prostor

tenzorski produkt vektorskih prostora

ortonormirana baza = $\{ |00\dots0\rangle, |00\dots1\rangle, |00\dots10\rangle, \dots, |11\dots1\rangle \}$ ← još pišem

$|10\dots0\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$

elemente identificiramo s brojevima $|0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle$ preko binarnog razvoja

$\otimes$ = tenzorski množenje - multilinearno preslikavanje

$$V \times V \times \dots \times V \longrightarrow V^{\otimes n}$$

$$(|i_1\rangle, |i_2\rangle, \dots, |i_n\rangle) \longmapsto |i_1\rangle \otimes |i_2\rangle \dots \otimes |i_n\rangle$$

npr. $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ i $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$

$$\Rightarrow |\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

$|0\rangle \otimes |0\rangle$

npr. $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

- Ne mogu se svi vektori iz prostora stanja ovako faktorizirati.

  Za qubite koji se nalaze u takvom nefaktoriziranom stanju kažemo da su kvantno spregnuti

Primjer/definicija mjerenja u sustavu od dva qubita.

Alice Bob imaju po jedan qubit

(pod-sustavi su izolirani)

- ako njihovi qubitovi nemaju interakciju (udaljeni nisu imali) onda se sustav nalazi u stanju $|\psi_1\rangle \otimes |\psi_2\rangle$ gdje su $|\psi_1\rangle$ i $|\psi_2\rangle$ vektori stanja svakog qubita posebno (stanje se može faktorizirati)
- općenito

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

gdje je $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

(režim prvi)

- Ako Alice izmjeri svoj qubit dobit će rezultat

$|0\rangle$ s vjerojatnošću $|\alpha_{00}|^2 + |\alpha_{01}|^2$

U tom slučaju, nakon mjerenja sustav prelazi i stanje

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

↖ faktorizirano stanje

mjerenjem se spregnutost uništava (ako ju postojala).

Slično i u drugom slučaju.